CUSTOMER PROPRIETARY

NETWORK INFORMATION

("CPNI")

PROTECTION POLICY

T3 Communications, Inc. (T3)

For More Information, Contact: Marshall Howard, 239-333-3035, M.Howard@t3com.net

Original Issue Date: December 1, 2007

Revised: January 18, 2013

Employees, contractors, agents, affiliates and partners of T3, including sales and marketing agents, are obligated to protect the confidentiality of customer information. Customer information obtained by T3 by virtue of its provision of telecommunications service may be considered Customer Proprietary Network Information ("CPNI"), and be subject to legal protection under Federal law and regulations. T3 supports these laws and regulations, and requires that its employees, contractors, agents, affiliates and partners comply with the policy set forth in this document.

See Glossary at the end of this document for meanings of underlined terms.

WHAT IS CPNI?

CPNI is defined by Federal statute:

> The term "customer proprietary network information" means—
>
> (A) information that relates to the quantity, technical configuration, type, destination, location and amount of use of a telecommunications service subscribed to by any customer of a telecommunications carrier, and that is made available to the carrier by the customer solely by virtue of the carrier-customer relationship; and
>
> (B) information contained in the bills pertaining to telephone exchange service or telephone toll service received by a customer of a carrier;
>
> except that such term does not include Subscriber List Information.
>
> 47 United States Code § 222(h)(1).

CPNI includes most information we collect about a customer because of their purchase of telecommunications services from us; this includes:

- Information about the ***types*** of service a customer buys, such as the technical configuration, destination and location of services a customer purchases from T3. This may include design layout reports, service addresses, originating and terminating locations, circuit speed and capacity, etc.

- Information about the ***amount*** of service a customer purchases from T3. For example, this may include the number of lines, circuits, calls, minutes, or the amount of equipment, subscribed to by the customer.

- Information about a customer's ***usage*** of telecommunications services, including numbers called, calls received, and optional features utilized.

- Information contained in a bill sent to the customer by T3.

CPNI does *not* include:

- Information that was not obtained by T3 by virtue of its carrier-customer relationship with the customer. For example, market information that the company may purchase from an outside source that happens to include data concerning one of T3's customers. However, information we obtain from aT3 affiliate that also provides service to a customer is deemed to be CPNI.

- Subscriber List Information. This is defined term under Federal law, and it means any information of a T3 subscriber (such as name, address, telephone number or classification) that the company or an affiliate has published, caused to be

published, or accepted for publication in a directory***. Non-published listings are considered CPNI.***

RESTRICTIONS ON USE OF CPNI

How may CPNI be used *without* the customer's approval?

- CPNI may always be used to provide the telecommunications service that the customer has purchased (such as customer service and repair), or to provide services necessary to, or used in, the provision of such telecommunications services, including the publishing of directories.

- T3 may use CPNI, without notice or approval, to bill and collect for services rendered, and to protect the company's rights and property (including fraud control).

- Aggregate Customer Information may be used without restriction. However, if the company uses Aggregate Customer Information for purposes other than providing telecommunications services, it must make the same aggregate information available to other parties upon request, on reasonable and non-discriminatory terms and conditions.

- For wire line service, CPNI may be used, without notice or customer approval, for the provision of customer premise equipment ("CPE"), call answering, voice mail or messaging, voice storage and retrieval services, fax storing and forwarding services and protocol conversion.

    - For wireless service providers, CPNI may be used for the provision of CPE and information service, and to provide call location information concerning the user of a commercial mobile service in association with the delivery of emergency services.

- CPNI may be used, without notice or approval, for marketing T3's services within a category of services to which the customer already subscribes. as the FCC recognizes three (3) categories of telecom services: local, inter-exchange and CMRS (mobile wireless) service. Therefore, if a customer already subscribes to T3's local service, the company may, without notice or approval, use that customer's CPNI for the purpose of marketing additional local services (but not inter-exchange or CMRS service).

- CPNI may be used to assist with any inbound telemarketing or administrative service for the duration of the customer's call, if the customer orally approves use of CPNI in this manner.

How may CPNI be used *with* the customer's approval?

- **T3 has chosen not to release or use CPNI for marketing purposes. This section is for information purposes only**.

- CPNI may be used to market T3's Communications-Related Services, and may be disclosed to T3's affiliates, as well as the company's third-party agents and joint venture partners providing Communications-Related Services, if the customer has received notice and has given approval by the "opt out" procedure. (*See* page 5). Specific requirements apply to how customer notices must be given (*see* pages 5-6), and the rules pertaining to "opt out" approval must be closely observed.

- CPNI may be disclosed to unrelated third parties and affiliates that *do not* provide Communications-Related services *only* if the customer's consent is obtained by the "opt in" procedure. (*See* page 5).

When is the company *required* to disclose CPNI?

- T3 must provide CPNI to any person designated by the customer, upon receipt of an affirmative written request from the customer. In general, the company cannot encourage a customer to freeze third-party access to CPNI.

- When required by law. **All such subpoenas, warrants, and similar requests for information should be directed to T3's Regulatory or Finance department.**

HOW T3 OBTAINS APPROVAL

FROM A CUSTOMER TO USE CPNI

T3, as we do not use CPNI to currently market our services, has limited needs for customer approval to use CPNI. For information purposes, the two methosds for obtaining approval are listed below.

Opt Out

- The "opt out" approval method requires that the customer receive an individual notice (by written or electronic means) that the company intends to use the customer's CPNI. Such notices must be sent by the company 30 days before the customer's approval to use CPNI is inferred (33 days for notices sent by mail). If the customer communicates to T3 that use of the CPNI is not approved, the company will honor that customer's decision to "opt out." In limited cases, oral approvals may be allowed, as described below in the section entitled *Special Requirements Applicable to One-Time Oral Notices to Customers.*

- If the company elects to send opt out notices by e-mail, the customer must previously have agreed to receive e-mails regarding their account. The subject line of the e-mail must clearly and accurately identify the topic, and the customer must have the option of replying directly to the e-mail. If the e-mail is returned as undeliverable, T3 may be not use the customer's CPNI until the required notice is given by another means. The customer must be able to opt out at no cost and be able notify the company of his or her decision on a 24-hour/7-day-per-week basis.

    - **Opt out approval must be refreshed every two years by sending a new notice, with a new 30 or 33 day waiting period for approval.**

Opt In

- This method requires T3 to obtain from the customer an affirmative, express consent--in oral, electronic or written form--allowing the requested CPNI usage, disclosure or access, after receiving appropriate notification.

- Although customer approvals under the opt in method may be obtained orally, T3 allows oral approvals only with written authorization of the company's management. If oral approval is received, the burden will lie on the company to show that the customer received all of the information that would otherwise have been required in writing, and gave the necessary approval.

Notice Requirements Applicable to both the Opt In and Opt Out Methods of Approval

- Notices to customers must be clearly written, legible, and provide sufficient information to enable the customer to make an informed decision to allow or deny use of CPNI. The company must describe what CPNI is, how it is proposed to be used by the company, and what specific entities may receive the CPNI if approval is granted. Although the notice may advise the customer that use or disclosure of CPNI will enhance T3's ability to provide services to the customer, the notice must also state that the customer has the right, and T3 has the duty under Federal law, to protect the confidentiality of CPNI. The customer must be informed of his or her right to deny or later withdraw approval of T3's proposed use of CPNI, and also be advised of the precise steps that must be taken in order to grant or deny approval of such use. Customers must be notified that denial of access to CPNI will not affect the provision of any services to which the customer subscribes.

Special Requirements Applicable to One-Time Oral Notices to Customers

- In general, one-time oral notices are appropriate when the company has made a one-time inbound or outbound telephone contact with the customer and access to CPNI is useful to analyze the customer's existing service. In such cases, T3 may use oral notices to obtain limited, one time use of CPNI only for the duration of the call, irrespective of whether the company uses opt-out or opt-in approval with respect to that customer. When using the one time oral notice method, the customer must be advised of the same information that would otherwise be provided in a written or electronic notice. However, certain information may be omitted from the oral notice, if it is clearly inapplicable, including: (a) notice that CPNI will be shared with affiliates or third parties; (b) the specific steps are necessary to approval or restrict use of CPNI; and (c) previous opt-out decisions require no further action to maintain the opt-out election. Notation should be made in the customer's record of any one-time oral notice to the customer and the customer's acceptance or rejection of one-time use of CPNI.

To avoid any doubt, prior to marketing any services to customers request permission to use CPNI even if the permission may not be required.

Always ask permission!

HOW TO VERIFY A CUSTOMER'S APPROVAL AND OBTAIN SUPERVISORY APPROVAL FOR PROPOSED OUTBOUND MARKETING EFFORTS

T3 does not at this time use CPNI for any outbound marketing. This section is informational only.

CUSTOMER APPROVAL DATABASE

- Upon implementation of a CPNI approval program, T3 will maintain a database that identifies whether or not a customer has given approval for access to its CPNI. Employees, contractors, agents, affiliates and partners of the company, including sales and marketing agents, are obligated to use that database before using, disclosing or permitting access to customers' CPNI. It is anticipated that such database will be customized to each employees individual job functions needs.

SUPERVISORY REVIEW REQUIRED BEFORE MAKING A REQUEST FOR CUSTOMER APPROVAL

- Employees, contractors, agents, affiliates and partners of the company, including sales and marketing agents, must obtain supervisory review before making any request to a customer to use, disclose or permit access to CPNI. All requests for such review should be directed to the VP of Sales, unless a unit supervisor has received prior authority to conduct such reviews. The review shall ensure that the requirements of this policy statement are adhered to. Note that Customer service, collections, and inbound sales representatives can request CPNI consent verbally on inbound calls from Customers without supervisory approval.

CONFIDENTIALITY AGREEMENTS WITH CONTRACTORS AND JOINT VENTURERS

T3 will share CPNI with a partner, contractor or agent only after that person or entity has entered into a confidentiality agreement with the company. The confidentiality agreement must include the following:

- Require that the partner, contractor or agent use the CPNI only for the purpose of marketing or providing the Communications-Related Services for which it was provided;

- Disallow the partner, contractor or agent from using, allowing access to or disclosing the CPNI to any other party, unless required to make such disclosure under force of law; and

- Require that the partner, contractor or agent have appropriate protections in place to ensure the ongoing confidentiality of the customer's CPNI.

All such agreements must be approved by a T3 VP or a T3 officer.

Employees are encouraged to request nondisclosure agreements from any contractor who may have access to CPNI data. If you have any questions about this, please ask.

RETENTION AND WIN-BACK

Restrictions on use of Carrier Proprietary Information to retain customers.

- If the company learns by receipt of another carrier's order to switch the customer, or another carrier's change request, that a customer plans to switch from T3 to another carrier, T3 prohibits its employees, agents, contractors or affiliates from using that information to attempt to dissuade the subscriber from leaving.

- It is specifically prohibited to access call records for the purpose of identifying customers who may have called or been called by any of our competitors.

- Subject to this policy statement on use of CPNI, if the company learns that a customer is switching to another carrier through an independent source (*e.g.*, from a communication received directly from the customer), CPNI may be used to persuade the customer to stay. All notice and consent requirements must be observed

Win-back

- Subject to this policy on use of CPNI, T3 encourages marketing campaigns to win back former customers that have switched to other carriers. If CPNI is used as part of a "win-back" campaign, all notice and consent requirements must be observed.

T3 does not use CPNI in its win-back campaigns. All employees will request one-time verbal approval before initiating any discussion with customers regarding retention or marketing of services.

HOW TO VERIFY A CUSTOMER'S APPROVAL TO RELEASE CPNI TO A CUSTOMER

SPECIFIC GUIDELINES GOVERNING DISCLOSURE OF CPNI TO CUSTOMERS

The FCC requires carriers to **authenticate** customers before releasing CPNI to them. **Authentication** means that carriers must objectively determine that customers are who they say they are before disclosing CPNI. This ensures that sensitive, private information is given only to the true customers, not pretexters. The type of authentication required varies based on the customer's method of communicating with the carrier: telephone, online, in person, mail.

Authentication for Release of Call Detail Records

Release of **Call Detail Information** CPNI to the Customer requires T3 to **authenticate** the identity of the Customer using any of the following methods:

1. **T3 may verify identity by calling the customer at the telephone number of record to disclose CPNI.**
   - Caller ID is not a valid method of confirming identity
   - If the customer cannot be reached at the telephone number of record, CPNI cannot be disclosed without an alternate method of authentication.

2. **T3 may mail CPNI information to the customer's bill address of record.**
   CPNI data (typically a reprint of the customer's bill or a new Password) may be sent to the bill address of record.
   - "Address of record" can be postal or electronic
   - Address must have been associated with the customer's account **for at least 30 days**

3. **T3 may release CPNI information to a customer in person after verifying the customer's identity through government-issued photo identification.**
   - ID must match the holder of the ID
   - ID must tie to listed name on the account
   - ID must be current
   - Student ID is **not** an acceptable form of ID

4. **T3 may disclose CPNI information to a customer who provides a previously established password.**
   - Passwords cannot include biographical data such as SSN, Student ID #, mother's maiden name or address or account information.
   - Establishment of a password requires that T3 first authenticate the Customer.
   - A random Password number can be used to initially establish a password

T3 may discuss CPNI information on a single event (usually a specific toll or long distance call) Without Authentication if the customer volunteers the CPNI information.

Absent authentication however T3 is not permitted to discuss other CPNI beyond the limited single event.

Authentication Exclusions (for Call Detail Records)

Authentication of the customer cannot be based on the following:

Readily available biographical information
- social security number, or the last four digits of that number;
- mother's maiden name;
- a home address; or
- date of birth

Account information
- phone number;
- membership ID; or
- amount of last bill

Special Exemptions for Business Accounts

T3 is exempted from the authentication rules if the communications-related service contract meets all of the following criteria:

(i) is with a business customer,
(ii) is serviced by a dedicated account representative as the primary contact, and
(iii) specifically addresses the carrier's protection of CPNI.

In these cases, the authentication rules are superseded by the service contract.

The business customer exemption only applies to business customers who may reach its designated customer service representative without going through a call center. Even where this exception applies, carriers are still subject to their general duty to protect CPNI, as well as the FCC's other rules not pertaining to customer authentication.

Any questions on how to serve a business customer should be addressed to your supervisor

Authentication via Passwords

FCC Rules allow T3 to establish a Password as a method of authentication of the Customer prior to releasing CPNI data.

1. **Passwords may be established in the initial provisioning of the account or at any time during the life of the account.**
   - Password assignment or release requires **authentication**.
   - Authentication on new Passwords:
     - In person with a government ID
     - Mailing to the address of record
     - Calling the Customer at the telephone number of record
   - Authentication for a change in Password can be done by using the current Password.

2. **T3-initiated Passwords do not rely on biological data**
   - Account number, SSN # or name-based Passwords are not permitted
   - Best option is a combination of numbers and letters

3. **T3 encourages the Customer to change his password**
   - T3 will allow the customer to reset the Password to something more memorable but will discourage Passwords that utilize account or personal information.
   - T3 will never suggest the customer establish a Password that follows biological pattern:

NO:	"We suggest you use your initials plus the last 4-digits of your phone number as your Password."
YES:	"We suggest you pick a date that is important to you plus a word you'll remember."

4. **If an on-line password is in place (*See Online Account Access)* and that password meets Password criteria, it may be used as an authenticating password for over the phone release on information**

5. **A change of Password either by T3 or the customer requires notice to the customer. *See Customer Notices following a Change in Account.***

Security Questions for the Recovery of Lost or Forgotten Passwords

T3 permits customers to establish a "recovery" question that would allow T3 to release or reset a Password or Password in the event the customer cannot remember the Password / Password. Such recovery question cannot include biological or account data. Possible questions include:

- Favorite childhood pet's name
- Favorite song / musician / movie / author
- Favorite hobby
- Country I'd most like to visit
- Person I'd most like to meet
- City where met current spouse
- Farthest from home traveled
- Question of the customer's choosing

T3 has offered customers the opportunity to select up to three recovery questions.

Warning: A Recovery question is essentially an authentication method that will permit ready access to CPNI. It should not rely on readily available biological data.

Absent a recovery question, T3 must utilize a different authentication method (mailing of a new Password, calling the customer at the number of record, or in person with an ID) to modify or reset Passwords.

Authentication for Release of Other Types of CPNI Data (non CDRs)

Safeguarding CPNI Telecommunications carriers must take reasonable measures to discover and protect against attempts to gain unauthorized access to CPNI. Telecommunications carriers must properly authenticate a customer prior to disclosing CPNI based on customer-initiated telephone contact, online account access, or an in-store visit.

At this time, federal statutes still allow for disclosure of CPNI related to all but call detail records using any of the authorization forms described previously (for CDRs) but also "reasonable" efforts to authenticate the customer.

Following are authorizations that may be used for the release of other information

T3 may disclose CPNI except call detail records using **reasonable** methods including:

- Last amount paid
- Other users listed on accounts
- Last service order
- Credit card number used to secure the account
- *Questionably SSN*

ATTENTION

If the conversation with the customer involves the disclosure of Call Detail Records you must **authenticate** the customer using the specific authentication options defined here.

Do not confuse "reasonable" authentication effort with authentication for purposes of release of call detail records.

Customer Notices following a Change in Authentication Method

Any change in an authenticating method on the customer's account requires T3 to issue a notice of change to the subscriber at the billing address or, in cases of change in billing address, to the prior billing address.

Such changes include:
- Change of password
- Change of billing address
- Addition of authorized users

Changes do not include:
- Changes in local services and features (**Note:** this does not pre-empt a carrier's requirement for other notices such as a notice regarding the removal of toll blocking)
- Billing adjustments that do not modify authentication.

Format for Notices:
- Notices must be "generic". They may reference the change in authentication has occurred but may not specify what change has occurred.
- Notice must be "immediate".
- Notice may be provided via call to the number of record
- Notice may also be mailed (or emailed) to the address of record *however* that address must have been established for 30 days. It is therefore concluded that mailing of notices regarding change in service address must be sent to the prior address or via a phone call.

Customer questions following a notice:

T3 may disclose the nature of the change described in the notice following authentication. Any question from the customer regarding the validity of a change should be referred to the compliance officer or a supervisor for handling.

Online Account Access

1. **General duty. Carriers are required to password protect online access to CPNI.** Password protection for online account access is subject to the same restrictions used in establishing passwords to discuss CPNI over the phone:
   - the carrier may not authenticate customers based on readily available biographical information
   - Authentication for the establishment of online passwords can be done using a previously-established Password; calling the telephone number of record, mailing the address of record, or in-person authentication
2. **Establishing / Changing Passwords**
   - Passwords may be established in the initial provisioning of the account or at any time during the life of the account.
     - The customer may establish his own Password following **authentication**.
     - T3 may assign a Password for the customer and provide the Password number to the customer following authentication of the customer (including mailing of the Password number to the address of record)
   - T3 may determine the format and length of passwords and may also block attempts to access the account after several failed password attempts.
   - T3 may choose to allow the customer to reset the Password to something more memorable but should avoid permitting Passwords that can easily reset by the customer or T3 to a Password that utilizes account or personal information. Generally, this means the Password should require a combination of numbers and letters.
   - A change of Password either by T3 or the customer requires notice to the customer. S*ee Customer Notices following a Change in Account***.**

TRAINING, REPORTING AND RECORD KEEPING

TRAINING REQUIREMENTS

- T3 will train all its employees, contractors, agents, affiliates and partners of the company, including sales and marketing agents, in the proper uses of CPNI, including a familiarity with this policy statement. Training will be repeated or refreshed as needed to insure all employees and contractors are aware of and compliant with CPNI requirements.

REPORTING REQUIREMENTS

- T3's CPNI administrator, Dan Lamey, is responsible for all government reporting requirements in connection with CPNI.

- T3 will provide a written report to the Federal Communications Commission ("FCC") of any instance in which the opt out method has failed to work properly, to such a degree that consumers' inability to opt out is more than an anomaly. The company's report will be filed with the FCC within five business days after learning of such failure. Any employee who becomes aware of any malfunction in the opt out system should immediately report it to their supervisor, T3's HR department, or CPNI administrator.

RECORD-KEEPING REQUIREMENTS

- T3 will maintain records of approval, whether oral, written or electronic, for a minimum of one year. A customer's approval or disapproval will remain in effect until the customer revokes or limits such approval or disapproval.

Notices Following a Violation of CPNI Rules

Upon discovery or suspicion of a CPNI Rule violation, the employee should promptly report the violation to the compliance officer with as much detail as possible. *See also Reports of Breach of CPNI data.*

a. Reports to Law Enforcement

Carriers *must* report CPNI breaches to law enforcement no later than seven (7) business days after a reasonable determination of a breach, by sending electronic notification through a central reporting facility to the United States Secret Service ("USSS") and the Federal Bureau of Investigation (FBI). The FCC has stated that it will maintain a link to the reporting facility at http://www.fcc.gov/eb/CPNI/.

b. Customer notification

T3 *may* notify the customer and/or disclose the breach publicly no sooner than seven (7) business days following notification to the USSS and the FBI and then only if the USSS and the FBI have not requested that the carrier continues to postpone disclosure. (If public disclosure would impede or compromise a criminal investigation, the law enforcement agency may direct the carrier to not disclose the breach for an initial 30-day period, which may be extended once as reasonably necessary in the judgment of the agency.)

Note that if T3 determines a breach has been made that significantly impairs or endangers a customer or group of customers it may notify authorities and request immediate notification.

Despite the temptation to do so, CPNI rules require that the customer **not** be notified of the breach of CPNI prior to notification schedule defined here without approval from the appropriate law enforcement agency.

Annual Certification Requirement

T3 must file an annual CPNI certification with the FCC on or before March 1 for data pertaining the previous year. T3 must be sure to comply exactly with the FCC's requirements, as the FCC's recent orders indicate that it will demand strict compliance with these requirements.

Critical inclusion:

- Officer of the company
- Must confirm "personnel knowledge" of steps taken to protect CPNI
- Must certify that the company has established operating procedures to protect CPNI
- Must cover all companies
- List all actions taken against data brokers
- Summarize all customer complaints regarding disclosure of CPNI
- Include a copy of CPNI policy

GLOSSARY

"Aggregate Customer Information" means collective data that relates to a group or category of services or customers, from which individual customer identities and characteristics have been removed

"Customer Proprietary Network Information (CPNI)" means (a) information that relates to the quantity, technical configuration, type, destination, location and amount of use of a telecommunications service subscribed to by any customer of a telecommunications carrier, and that is made available to the carrier by the customer solely by virtue of the carrier-customer relationship; and (b) information contained in the bills pertaining to telephone exchange service or telephone toll service received by a customer of a carrier; except that such term does not include subscriber list information.

"Carrier Proprietary Information (CPI)" means a request from one carrier to another to *switch* a customer.

"Communications-Related Services" means telecommunications services, information services typically provided by telecommunications carriers, and services related to the provision and maintenance of customer premises equipment. Information services that are typically provided by telecommunications carriers include Internet access and voice mail services. Retail consumer services provided by use of Internet websites (such as travel reservation services or mortgage lending services), are not typically provided by telecommunications carriers and are not considered to be Communications-Related Services, whether or not such services may otherwise be considered to be information services.

"Subscriber List Information" means any information of a T3 subscriber (such as name, address, telephone number or classification) that the company or an affiliate has been published, caused to be published, or accepted for publication in a directory.

"Telecommunications Carrier or Carrier" has the meaning set forth in Section 3(44) of the Communications Act of 1934, as amended. Generally, a telecommunications carrier is a provider of transmissions services directly to the public for a fee, between or among points specified by the user, without change in the form or content of the information as sent and received.T3 is a telecommunications carrier.